# McAfee Enterprise Security Manager

**Prioritize. Investigate. Respond.**

The most effective security starts with visibility into all activity on systems, networks, databases, and applications. Security information and event management (SIEM) is the foundation of an effective security framework. McAfee® Enterprise Security Manager, the core of the McAfee SIEM solution, delivers performance, actionable intelligence, and solution integration at the speed and scale required for security organizations. It allows you to quickly prioritize, investigate, and respond to hidden threats and meet compliance requirements.

McAfee Enterprise Security Manager delivers a real-time understanding of the world outside—threat data and reputation feeds—as well as a view of the systems, data, risks, and activities inside your enterprise. It offers your security team complete and correlated access to the content and context needed for fast, risk-based decisions, so you can invest resources to best effect in a dynamic threat and operational landscape. This is critical for investigating "low-and-slow" attacks, searching for indicators of compromise (IoCs), or remediating audit findings. To make threat and compliance management an integral part of security operations, McAfee Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized policy management—everything you need to improve workflow and security operations team efficiency. Additionally, Content Packs available for McAfee Enterprise Security Manager offer prebuilt configurations for advanced security use cases that help simplify security operations.

## Built for Enterprise Scale

Security operations teams increasingly require greater efficiency as they collect and rapidly explore increasingly large volumes of raw and parsed data from today's dynamic and distributed enterprise architectures. To overcome this challenge, McAfee Enterprise Security Manager uses an open and scalable data bus that was built specifically for high-volume data processing. In addition, a highly scalable data architecture supports ingestion, management, and analysis to prevent compromises to data collection, searching, and retention. Such compromises can jeopardize investigations when critical data is not available later, when query response slows analysis, or when only partial searching is possible due to performance.

## Key Advantages

- **Intelligent:** Advanced analytics and rich context help you detect and prioritize threats.
- **Actionable:** The data you need is presented in dynamic views that include the option to take action to investigate, contain, remediate, and adapt to important alerts and patterns.
- **Integrated:** The solution monitors and analyzes data from a broad heterogeneous security infrastructure and offers two-way integration via open interfaces. It also allows many first response actions to be automated.

Connect With Us

## Critical Facts in Minutes, Not Hours

Rapid access to long-term storage of event data is critical for investigating incidents, searching for evidence of advanced attacks, or attempting to remediate a failed compliance audit—all of which require visibility into historical data and full access to the complete details of each specific event.

Highly tuned appliances can collect, process, and correlate log events from multiple years with other data streams, including STIX-based threat intelligence feeds, at the speed you require. McAfee Enterprise Security Manager is able to store billions of events and flows, keeping all information available for immediate ad hoc queries, while retaining data long term for forensics, rules validation, and compliance. Moreover, data can be replicated to multiple storage locations immediately, maintaining business continuity.

## Context and Content Awareness

When contextual information is available—including threat data and reputation feeds, identity and access management systems, privacy solutions, or other supported systems—each event is enriched with that context. This enrichment delivers better understanding and accurate triage based on how network and security events correlate to asset attributes and real business processes and policies.

McAfee Enterprise Security Manager's scalability and performance enable collection of more information from more sources, including application content, such as documents, transactions, and communications, providing deep forensic value to you. This information is heavily indexed, normalized, and correlated to help you detect a wider range of risks and threats.

## Advanced Threat Interpretation

Whether it is network traffic, user activity, or application use, any variation from normal activity could indicate that a threat is imminent and that your data or infrastructure is at risk. McAfee Enterprise Security Manager calculates baseline activity for all collected information and provides prioritized alerts with the goal of discovering potential threats before they occur, while at the same time analyzing that data for patterns that may indicate a larger threat. In addition, McAfee Enterprise Security Manager leverages contextual information and enriches each event with that context for a better understanding of how security events can impact real business processes.

McAfee Enterprise Security Manager's Cyber Threat Management dashboards offer enhanced real-time monitoring and understanding of emerging threats. Suspicious or confirmed threat information reported via STIX/TAXII, McAfee Advanced Threat Defense, and/or third-party web URLs can be aggregated and correlated in near real time or historically (using the backtrace feature) against event data, providing security teams with a deeper understanding of the threat propagation within an environment. This intelligence enables organizations to align the right data with the right people to take action in near real time and make smarter decisions.

## Optimize Security Operations

McAfee Enterprise Security Manager's analyst-centric user experience offers increased flexibility, ease of customization, and faster response to investigations. Streamlined workflows allow for more timely and effective incident management. With fast and smart access to threat information, analysts with any level of expertise—from beginner to expert—will find it easier to prioritize, investigate, and respond to evolving threats.

The usability of McAfee Enterprise Security Manager starts right out of the box, with hundreds of reports, views, rules, and alerts to use immediately—and all are easily customizable. Whether setting up baselining for understanding typical network usage or simply customizing alerts, McAfee Enterprise Security Manager's dashboard enables easy visualization, investigation, and reporting on the most relevant security information. Now, organizations can have comprehensive and correlated access to the data and context needed for making fast and smart decisions.

In addition, McAfee Enterprise Security Manager offers Content Packs to simplify security operations with "ready-to-go" security use cases that are preconfigured and offer fast access to advanced threat or compliance-management capabilities. Content Packs are prebuilt configurations for common security use cases that provide sets of rules, alarms, views, reports, variables, and watchlists. Many Content Packs provide prepackaged triggers for behaviors that may warrant additional scrutiny or automatic remediation.

## Simplify Compliance

By centralizing and automating compliance monitoring and reporting, McAfee Enterprise Security Manager eliminates time-consuming manual processes. Additionally, integration with the Unified Compliance Framework (UCF) enables a "collect-once, comply-with-many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum. Support for the UCF brings efficiencies to compliance by normalizing the specifics of each regulation, which enables the single set of collected events to be easily mapped to the individual regulations.

McAfee Enterprise Security Manager makes compliance management easy and fast with hundreds of prebuilt dashboards, comprehensive audit trails, and reports for more than 240 global regulations and control frameworks, including PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, and SOX. Beyond the extensive out-of-the-box support, all McAfee Enterprise Security Manager compliance reports, rules, and dashboards are fully customizable.

## Connecting Your IT Infrastructure

Integration across your security infrastructure delivers an unprecedented level of real-time visibility into an organization's security posture. McAfee Enterprise Security Manager can collect valuable data from hundreds of third-party security vendor devices, as well as threat intelligence feeds. Integration with McAfee Global Threat Intelligence (McAfee GTI) brings in data from more than 100 million McAfee Labs global threat

sensors, offering a constantly updated feed of known malicious IP addresses. McAfee Enterprise Security Manager can also ingest threat information reported via STIX/TAXII and/or third-party web URLs and take action based on analysis.

McAfee Enterprise Security Manager also offers active integrations with dozens of complementary incident management and analytics solutions, including McAfee solutions and McAfee Security Innovation Alliance partner solutions.

For example, McAfee Threat Intelligence Exchange, based on endpoint monitoring, aggregates low-prevalence attacks, leveraging global, third-party, and local threat intelligence. McAfee Threat Intelligence Exchange can also utilize other integrated products, such as McAfee Advanced Threat Defense, to further analyze and convict files.

Analysts also benefit from integration with McAfee Behavioral Analytics, a dedicated user and entity behavior analytics solution that distills billions of security events down to hundreds of anomalies to produce a handful of prioritized threat leads and allows analysts to discover unusual and high-risk security threats, often unidentifiable by other solutions. Similarly, McAfee Enterprise Security Manager integrates with McAfee Investigator to help transform analysts into expert investigators and to allow them to close more cases faster with higher confidence that they have determined root cause.

Incident response teams and administrators can use McAfee Active Response to look for malicious zero-day files that lay dormant on systems, as well as active processes in memory. McAfee Active Response also uses persistent collectors to continuously monitor your endpoints for specific IoCs, automatically alerting you if an IoC appears somewhere in your environment. Unlike standard security approaches, this combination provides organizations with detailed, closed-loop workflow from discovery to containment and remediation.

McAfee delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. McAfee is committed to being your number one security partner, providing you with a complete set of integrated security capabilities.

## Learn More

For more information on McAfee Enterprise Security Manager, visit **www.mcafee.com/siem**.

For more information on integrated solutions, **www.mcafee.com/secops**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com